TRICARE Management Activity Brown Bag Series 2004

Overview of the HIPAA Security Rule

TMA Privacy Officer
TRICARE Management Activity
email: privacymail@tma.osd.mil

May 2004

Our Commitment to Security

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

TRICARE Management Activity

Presentation Objectives

- Provide an overview of the HIPAA Security Rule
- Explain HIPAA Security components
- Describe TMA efforts to aid implementation of the standards

What Is HIPAA?

Health Insurance Portability and Accountability Act (HIPAA)

Public Law 104-191 enacted August 21, 1996

- Improve portability & continuity of health insurance coverage
- Improve access to long term care services and coverage
- Simplify the administration of health care

Rule Background

Administrative Simplification Subtitle includes Four Rules

- Transactions and Code Sets
- Privacy
- Security
- Identifiers

Compliance Date for Security is April 21, 2005

What Information is Protected?

Electronic Protected Health Information (EPHI)

- Individually identifiable health information (including demographics) in electronic form
- Held by health plans, healthcare providers or their business associates

Any health information that identifies you as you and is in electronic form

HIPAA Security vs. HIPAA Privacy

Security

- Standards for how to protect EPHI
- Focus on confidentiality, integrity and availability
- Applies only to PHI in electronic format
- Through administrative, physical and technical safeguards

Privacy

- Standards for using PHI
- Focus on confidentiality
- Applies to PHI in any format
- Through use & disclosure rules and patient rights

Rule Objective

Implement reasonable and appropriate administrative, physical and technical safeguards to protect against any reasonably anticipated threats or hazards.

Rule Compliance

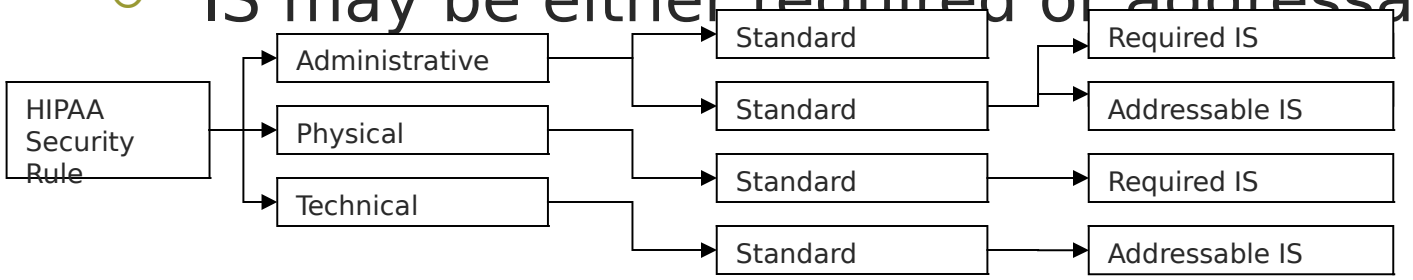
To correctly implement the security standards each covered entity must:

- Assess potential risks and vulnerabilities to EPHI;
- Develop, implement and maintain appropriate security measures given those risks; and
- Document those measures and keep them current

HIPAA Security is meant to be flexible and scalable.

Rule Structure

- Organized into three categories; Administrative, Physical and Technical
- Categories contain standards and associated implementation specifications (IS)
  - All standards are required
  - IS may be either required or addressable



What does “addressable” mean?

- Addressable IS must be assessed and reasonable and appropriate action taken based on results of:
  - Risk assessment
  - Mitigation strategy
  - Security measures already in place
  - Cost of alternatives
- Document action taken and rationale

HIPAA / DoD Policy

Comparisons between the HIPAA Rules and DoD Policy result in four possible combinations.

- HIPAA Required/DoD Required
- HIPAA Required/DoD Addressable
- HIPAA Addressable/DoD Required
- HIPAA Addressable/DoD Addressable

HIPAA / DoD Policy

- HIPAA Required / DoD Required
  - HIPAA requires Unique User Identification
  - DoD 8500.2-I requires Unique User Identification
- No action required other than verification and documentation of compliance

HIPAA / DoD Policy

- HIPAA Required / DoD Addressable
  - HIPAA requires Business Associate Agreements
  - DoD policy does not currently require business associate agreements that meet the requirements of HIPAA Security Rule
- DoD to develop policies to comply with the Business Associate Agreement standard

HIPAA / DoD Policy

- HIPAA Addressable / DoD Required
  - Applications/Data Criticality Analysis is Addressable in HIPAA
  - DoD requires Application/Data Criticality Analysis through DoD 8500.1-D, DoD 8500.2-I, and DoD 8510.1-M
- No action required other than verification and documentation of compliance

HIPAA / DoD Policy

- HIPAA Addressable / DoD Addressable
  - In HIPAA Encryption and Decryption of data at rest is addressable
  - DoD does not require Encryption and Decryption of sensitive data at rest
- Each Service component or MTF must assess the need to encrypt data at rest and document action taken or not taken and rationale

Standards - Administrative

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Security Evaluation
- Business Associate Contracts

Standards - Administrative

- Security management process
- Process used to implement the rest of the rule
- Foundation of security program
- Includes:
  - Risk analysis (R)
  - Risk management (R)
  - A sanction policy, and (R)
  - Information system activity review (R)

Standards - Administrative

- Assign security responsibility
- Implement workforce security program, including:
  - Authorization and/or supervision for all workforce members (A)
  - Workforce clearance procedures (A)
  - Termination procedures (A)

Standards - Administrative

- Implement an information access management plan including:
  - Isolation of healthcare clearinghouse functions (R);
  - Access authorization (A); and
  - Access establishment and modification (A

Standards - Administrative

- Develop a security awareness and training program, including:
  - Security reminders (A);
  - Protection from malicious software (A);
  - Log-in monitoring (A); and
  - Password management (A)
- Implement security incident procedures, including;
  - Response and reporting procedures (R)

Standards - Administrative

- Develop a contingency plan and implement as needed, including:
  - Data backup plan (R);
  - Disaster recovery plan (R);
  - Emergency mode operation plan (R);
  - Testing and revision procedures (A); and
  - Applications and data criticality analysis (A).

Standards - Administrative

- Perform periodic technical and non-technical evaluations
- Obtain satisfactory assurances that business associates will appropriately safeguard EPHI
  - The single required IS states contracts and agreements detailing the assurances must be in writing

Standards - Physical

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Standards - Physical

- Facility Access Controls - Limit physical access to the facility and electronic information systems
  - Contingency operations (A)
  - Facility security plan (A)
  - Access control and validation procedures (A)
  - Maintenance records (A)

Standards - Physical

"Workstation" includes any electronic device used to input and/or process health information such as laptops, personal computers or computer terminals.

- Workstation Use - Document the appropriate physical environment and use of workstations
- Workstation Security - Protect workstations from unauthorized access

Standards - Physical

Media includes drives (permanent and removable), diskettes, compact discs, tapes and any other device that is capable of storing electronic information

- Control the movement of devices and media
  - Disposal (R)
  - Media Re-use (R)
  - Accountability (A)
  - Data backup and storage (A)

Standards - Technical

- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Standards - Technical

- Implement technical access control policies and procedures that enforce administrative information access management policies
  - Unique user identification (R)
  - Emergency access procedure (R)
  - Automatic logoff (A)
  - Encryption and decryption (A)

Standards - Technical

- Install and use audit mechanisms
- Protect EPHI from unauthorized alteration or destruction
  - Mechanism to authenticate EPHI
- Install and use technical procedures that verify the identity of persons or “entities” requesting access to EPHI.

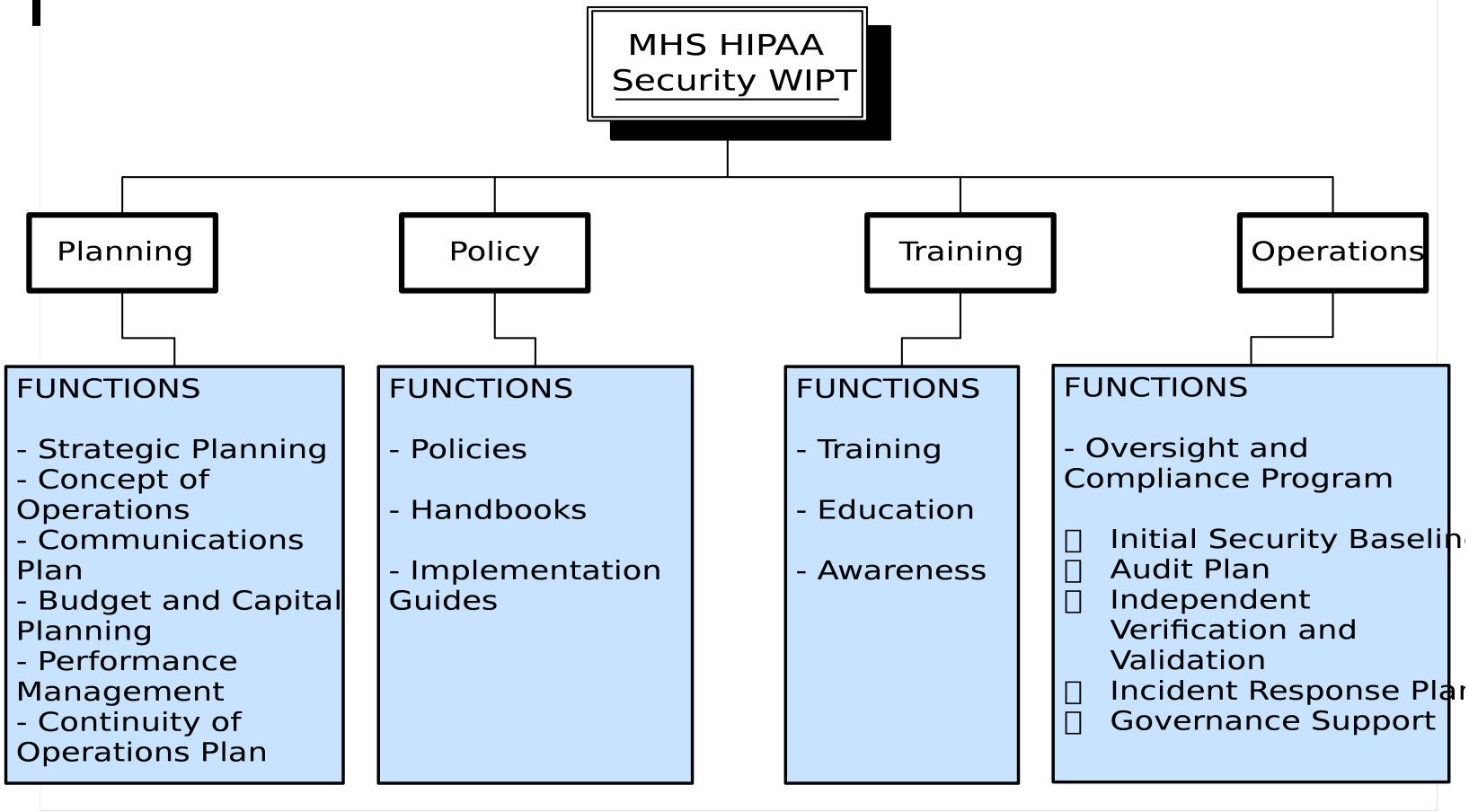
Standards - Technical

- Install technical controls to protect EPHI from unauthorized access during transmission
  - Integrity controls (A)
  - Encryption (A)

Policies, Procedures and Documentation

- Covered entities must implement “reasonable and appropriate” policies and procedures to comply with the standards and IS.
- Document all policies and procedures and any required action, activity or assessment.
  - Time limit (R)
  - Availability (R)
  - Updates (R)

MHS HIPAA Security WIPT



HIPAA Security

MHS HIPAA Security IPT

- Purpose: Provide methodology for implementation of the Security Rule.
- Planning Subcommittee
  - Design, develop, implement and monitor a MHS HIPAA Security Program
- Policy Subcommittee
  - Establish policy, responsibilities, procedures and best practices for DoD activities compliance

MHS HIPAA Security IPT

- Training Subcommittee
  - Provide all members of the MHS workforce with annual HIPAA compliance training
  - Provide specialized training to those with specific HIPAA responsibility
- Operations Subcommittee
  - Establish an Oversight and Compliance Program

TMA HIPAA Web site

- http://tricare.osd.mil/tmaprivacy/
  - Privacy and Security Guidance
  - Information papers
  - FAQs
- privacymail@tma.osd.mil
- https://rimr.tatrc.org/
  - P3WG Report

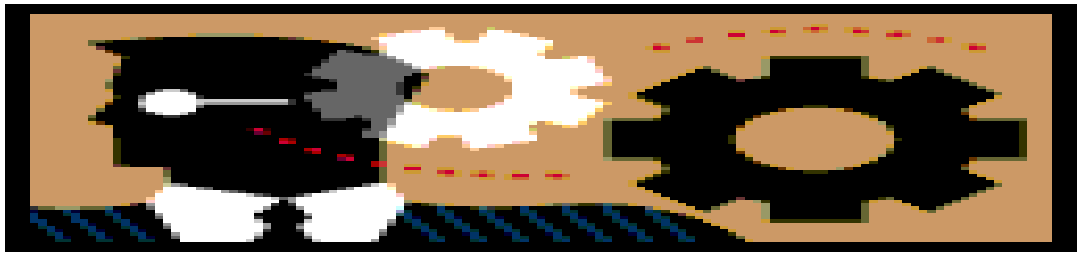
Our Commitment to Security

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

TRICARE Management Activity

QUESTIONS ?

QUESTIONS ?



QUESTIONS ?

QUESTIONS ?

QUESTIONS ?